

The Dual and the Gray Image of Codes over

$$\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$$

A. Melakheso and K. Guenda

Abstract

In this paper, we study the linear codes over the commutative ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and their Gray images, where $v^3 = v$. We define the Lee weight of the elements of R , we give a Gray map from R^n to \mathbb{F}_q^{3n} and we give the relation between the dual and the Gray image of a code. This allows us to investigate the structure and properties of self-dual cyclic, formally self-dual and the Gray image of formally self-dual codes over R . Further, we give several constructions of formally self-dual codes over R .

1 Introduction

Codes over finite rings have been studied since the early. There are a lot of work on this codes after the discovery of certain good non-linear codes can be constructed from cyclic codes over \mathbb{Z}_4 . Recently, Zhu et al. considered linear codes over finite non-chain ring $\mathbb{F}_q + v\mathbb{F}_q$, they investigated a class of constacyclic over $\mathbb{F}_p + v\mathbb{F}_p$ [8].

In [5] the authors studied cyclic codes and the weight enumerator of linear codes over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$.

In this paper, we focus on codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$. The remainder of the paper is organized as follows. In section 2, we give some basic knowledge about the finite ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. In section 3, we define the Lee weight of the element of R , and introduce a Gray map. This map leads to some useful results on linear codes over R . We investigated the relation between the dual and the Gray image of codes. In section we study cyclic codes over R . We finish by giving different constructions of formally self-dual and we study the Gray map of formally self-dual codes over R .

2 Preliminaries

In this section, we introduce some basic results on linear codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, q a prime power, where $v^3 = v$. An element x of R can be expressed uniquely as

$x = a_0 + va_1 + v^2a_2$, where $a_i \in \mathbb{F}_q, i = 0, 1, 2$. $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ is principal ideal ring and has three non-trivial ideals, namely,

$$\begin{aligned} \langle v \rangle &= \{a_1v; a_1 \in \mathbb{F}_q\}, \\ \langle 1 - v \rangle &= \{a_2(1 - v); a_2 \in \mathbb{F}_q\}, \\ \langle 1 - v^2 \rangle &= \{a_3(1 - v^2); a_3 \in \mathbb{F}_q\}. \end{aligned}$$

Let $(\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q)^n$ be the $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ -module of n -tuple over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. A linear code C of length n over R is an R -submodule of R^n . An element of C is called a codeword of C . A generator matrix of C is a matrix whose rows generate C . The Hamming weight $w_H(c)$ of codeword c is the number of nonzero components in c . The Hamming distance $d_H(C)$ of C is defined as $d_H = \min\{w_H(x_1 - x_2) \mid x_1, x_2 \in C, x_1 \neq x_2\}$. Let $x = (x_0, x_1, \dots, x_{n-1})$ and $y = (y_0, y_1, \dots, y_{n-1})$ be two element of R^n , the Euclidean inner product is given as:

$$x \cdot y = x_0y_0 + x_1y_1 + \dots + x_{n-1}y_{n-1}.$$

The dual code C^\perp of C with respect to the Euclidean inner product is defined as

$$C^\perp = \{x \in R^n \mid x \cdot y = 0, \forall y \in C\}.$$

C is self-dual if $C = C^\perp$, C is self-orthogonal if $C \subseteq C^\perp$ [9]. Let C be linear code of length n over R . Define

$$\begin{aligned} C_1 &= \{a \in \mathbb{F}_q^n; \exists b, c \in \mathbb{F}_q^n; a + vb + v^2c \in C\}, \\ C_2 &= \{a + b \in \mathbb{F}_q^n; \exists c \in \mathbb{F}_q^n; a + vb + v^2c \in C\}, \\ C_3 &= \{a + b + c \in \mathbb{F}_q^n; a + vb + v^2c \in C\}. \end{aligned}$$

Obviously, C_1 , C_2 , and C_3 are linear codes over \mathbb{F}_q .

By the definition of C_1 , C_2 , and C_3 we have that $C = vC_1 \oplus (1 - v)C_2 \oplus (1 - v^2)C_3$. So C_1 , C_2 and C_3 are unique. That we have $|C| = |C_1||C_2||C_3|$.

3 Gray Map over R

Let $x = a_0 + va_1 + v^2a_2$ be an element of R where $a_i \in \mathbb{F}_q, i = 0, 1, 2$.

We define Gray map Ψ from R to \mathbb{F}_q^{3n} by

$$\begin{aligned} \Psi : R &\rightarrow \mathbb{F}_q^{3n} \\ x = a_0 + va_1 + v^2a_2 &\mapsto \Psi(x) = (a_0, a_0 + a_2, a_1) \end{aligned}$$

From definition, the Lee weight of elements of R is defined as follows

$$w_L(a_0 + va_1 + v^2a_2) = \begin{cases} 0 & \text{if } a_0 = 0; \quad a_1 = 0; \quad a_2 = 0 \\ 1 & \text{if } a_0 = 0; \quad a_1 \neq 0; \quad a_2 = 0 \\ 1 & \text{if } a_0 \neq 0; \quad a_1 \neq 0; \quad a_2 = 0 \\ 1 & \text{if } a_0 \neq 0; \quad a_1 = 0; \quad a_0 + a_2 = 0 \pmod{q} \\ 1 & \text{if } a_0 = 0; \quad a_1 \neq 0; \quad a_2 \neq 0 \\ 2 & \text{if } a_0 \neq 0; \quad a_1 = 0; \quad a_0 + a_2 = 0 \pmod{q} \\ 2 & \text{if } a_0 = 0; \quad a_1 \neq 0; \quad a_2 \neq 0 \\ 2 & \text{if } a_0 \neq 0; \quad a_1 \neq 0; \quad a_0 + a_1 = 0 \pmod{q} \\ 3 & \text{if } a_0 \neq 0; \quad a_1 \neq 0; \quad a_0 + a_2 = 0 \pmod{q} \\ 3 & \text{if } a_0 \neq 0; \quad a_1 \neq 0; \quad a_2 = 0 \end{cases}$$

For any codeword $c = (c_0, c_1, \dots, c_{n-1})$ the Lee weight of c is defined as $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ and the Lee distance of c is defined as $d_L(c) = \min_{\hat{c}} d_L(c, \hat{c})$, where $d_L(c, \hat{c}) = w_L(c - \hat{c})$ for any $\hat{c} \in C$, $c \neq \hat{c}$.

Now can be extended the Gray map to R^n .

Definition 3.1 The Gray map Ψ from R^n to \mathbb{F}_q^{3n} is define $\Psi(a_0, a_1, a_2) = (a_0, a_0 + a_2, a_1)$ for all $a_i \in \mathbb{F}_q^{3n}$, $i = 0, 1, 2$.

Theorem 3.2 The Gray map Ψ is a weight preserving map from $(R^n, \text{Lee weight})$ to $(\mathbb{F}_q^{3n}, \text{Hamming weight})$.

Proof.

Let $c = (c_0, c_1, \dots, c_{n-1}) \in R^n$ and $\hat{c} = (\hat{c}_0, \hat{c}_1, \dots, \hat{c}_{n-1}) \in R^n$. Since $w_L(c) = w_H(\Psi(c_i))$, $i = 0, 1, \dots, n-1$, then we have

$$w_L(c) = \sum_{i=0}^{n-1} w_L(c_i) = \sum_{i=0}^{n-1} w_H(\Psi(c_i)) = w_H(\Psi(c)).$$

□

Theorem 3.3 If C is self orthogonal, so is $\Psi(C)$.

Proof. Let $c = a_1 + vb_1 + v^2c_1$, $\hat{c} = a_2 + vb_2 + v^2c_2$, where $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{F}_q$. And let

$$c \cdot \hat{c} = a_1a_2 + v(a_1b_1 + b_1a_2 + b_1c_2 + c_1b_2) + v^2(a_1a_2 + b_1b_2 + c_1a_2 + c_1c_2)$$

if C is self orthogonal, so we have $a_1a_2 = 0$, $a_1b_1 + b_1a_2 + b_1c_2 + c_1b_2 = 0$ and $a_1a_2 + b_1b_2 + c_1a_2 + c_1c_2 = 0$.

From

$$\Psi(c) \cdot \Psi(\hat{c}) = (a_1, a_1 + c_1, b_1)(a_2, a_2 + c_2, b_2) = a_1a_2 + a_1a_2 + a_1c_2 + c_1a_2 + c_1c_2 + b_1b_2 = 0.$$

Therefore, we have $\Psi(C)$ is self orthogonal. \square

Corollary 3.4 *If C is a linear code over R , the minimum Lee weight of C is the same as the minimum Hamming weight of $\Psi(C)$.*

Let d_L minimum Lee weight of linear code over R .

Then $d_L = \min \{d_H(C_1), d_H(C_2), d_H(C_3)\}$ where $d_H(C_i)$ denotes the minimum Hamming weight of codes, C_1, C_2 and C_3 .

Lemma 3.5 *Let $C = vC_1 \oplus (1-v)C_2 \oplus (1-v^2)C_3$ be a linear code over R , where C_i is a linear code with dimension k_i and minimum Hamming distance $d(C_i)$ for $i = 1, 2, 3$. Then $\Psi(C)$ is a linear code with parameters $[3n, k_1 + k_2 + k_3, \min \{d(C_1), d(C_2), d(C_3)\}]$ over \mathbb{F}_q .*

In the following we investigate the relation between the dual and the Gray image of a code over R .

Theorem 3.6 *If C^\perp is the dual of C , then $\Psi(C)^\perp = \Psi(C^\perp)$. Moreover, if C is self-dual code, so is $\Psi(C)$.*

Proof.

For all $c_1 = a_0 + va_1 + v^2a_2 \in C$ and $c_2 = \acute{a}_0 + \acute{a}_1v + \acute{a}_2v^2 \in C^\perp$, where $a_i, \acute{a}_i \in \mathbb{F}_q^n, i = 0, 1, 2$, if $c_1 \cdot c_2 = 0$, then we have

$c_1 \cdot c_2 = a_0\acute{a}_0 + v(a_0\acute{a}_1 + a_1\acute{a}_0 + a_1\acute{a}_2 + a_2\acute{a}_1) + v^2(a_0\acute{a}_2 + a_1\acute{a}_1 + a_2\acute{a}_0 + a_2\acute{a}_2) = 0$. Implying that $a_0\acute{a}_0 = 0, a_0\acute{a}_1 + a_1\acute{a}_0 + a_1\acute{a}_2 + a_2\acute{a}_1 = 0$, and $a_0\acute{a}_2 + a_1\acute{a}_1 + a_2\acute{a}_0 + a_2\acute{a}_2 = 0$. Therefore

$$\Psi(c_1) \cdot \Psi(c_2) = (a_0, a_0 + a_2, a_1) \cdot (a_0, \acute{a}_0 + \acute{a}_2, \acute{a}_1) = a_0\acute{a}_0 + a_0\acute{a}_0 + a_0\acute{a}_2 + a_2\acute{a}_0 + a_2\acute{a}_2 + a_1\acute{a}_1 = 0.$$

Thus $\Psi(C^\perp) \subseteq \Psi(C)^\perp$. From Lemma 3.5, we can verify that $|\Psi(C)^\perp| = |\Psi(C^\perp)|$, which implies that $\Psi(C)^\perp = \Psi(C^\perp)$.

Clearly, $\Psi(C)$ is self-orthogonal if C is self-dual. However $|\Psi(C^\perp)| = |\Psi(C)^\perp| = q^{3n-k_1-k_2-k_3}$. Hence $\Psi(C)$ and $\Psi(C^\perp)$ are dual \mathbb{F}_q -linear codes. \square

4 The Weight Enumerators of Linear Codes over R

One of the most important results in coding theory is that MacWilliams identity that describes the connections between a linear code and its dual on the weight enumerator, so we investigate this question over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$.

Let C be a linear code of length n over R . Suppose that a is an element of R . For all $c = (c_0, c_1, \dots, c_{n-1}) \in R^n$, define the weight of c at a to be $w_a = |\{i \mid c_i = a\}|$.

Definition 4.1 Let E_i be the number of codewords of Lee weight i in C . Then $\{E_0, E_1, \dots, E_{3n}\}$ is called the Lee distribution of C .

Define the Lee weight enumerator of C as $Lee_C(X, Y) = \sum_{c \in C} E_i X^{3n-i} Y^i$. Clearly, $Lee_C(X, Y) = \sum_{c \in C} X^{3n-w_L(c)} Y^{w_L(c)}$. Furthermore, the complete weight enumerator of C over R is usually denoted by

$$cwe_C(X_0, X_1, \dots, X_{(q-1)^3}) = \sum_{c \in C} \left(X_0^{w_{g_0}(c)}, X_1^{w_{g_1}(c)}, \dots, X_{q^3-1}^{w_{q^3-1}(c)} \right)$$

We denote $\eta a_0 = 0, \eta_1 = a_0, \eta_2 = a_1v, \eta_3 = a_2v^2, \eta_4 = a_0 + a_1v, \eta_5 = a_0 + a_2v^2, \eta_6 = a_1v + a_2v^2, \eta_7 = a_0 + a_1v + a_2v^2$, where $a_i \in \mathbb{F}_q, i = 0, 1, 2$.

For any codeword c of C , let

$$\begin{aligned} \alpha_0(c) &= w_{\eta_0}(c) \\ \alpha_1(c) &= w_{\eta_3}(c) + w_{\eta_4}(c) + w_{\eta_6}(c) + w_{\eta_7}(c) \\ \alpha_2(c) &= w_{\eta_1}(c) + w_{\eta_4}(c) + w_{\eta_5}(c) + w_{\eta_6}(c) \\ \alpha_3(c) &= w_{\eta_4}(c) + w_{\eta_5}(c) + w_{\eta_7}(c) \end{aligned}$$

The Lee weight $w_L(c)$ of c is defined to be

$$w_L(c) = \alpha_1(c) + 2\alpha_2(c) + 3\alpha_3(c).$$

We define

$$\begin{aligned} swe_C(X_0, X_1, X_2, X_3) &= cwe_C(X_0, X_1, \dots, X_{q^3-1}) \\ &= \sum_{c \in C} X_0^{\alpha_0(c)} X_1^{\alpha_1(c)} X_2^{\alpha_2(c)} X_3^{\alpha_3(c)}. \end{aligned}$$

The Hamming weight enumerator of a code C of length n is defined to be

$$Ham_C(X, Y) = \sum_{c \in C} X^{n-w_H(c)} Y^{w_H(c)}$$

Theorem 4.2 Let C be linear code over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, then

$$1. Lee_C(X, Y) = cwe_C(X^3, X^2Y, XY^2, Y^3).$$

2. $Ham(X, Y) = cwe_C(X, Y, Y, Y).$
3. $Lee_C(X, Y) = w_{\Psi(C)}(X, Y).$
4. $Lee_{C^\perp}(X, Y) = \frac{1}{|C|} Lee_C(X + Y, X - Y).$

Proof.

1. From the definition of the symmetrized weight enumerator, we have

$$\begin{aligned}
cwe_C(X^3, X^2Y, XY^2, Y^3) &= \sum_{c \in C} X^{3\alpha_0(c)} (X^2Y)^{\alpha_1(c)} (XY^2)^{\alpha_2(c)} (Y^3)^{\alpha_3(c)} \\
&= \sum_{c \in C} X^{3\alpha_0(c)} X^{2\alpha_1(c)} Y^{\alpha_1(c)} X^{2\alpha_2(c)} Y^{2\alpha_2(c)} Y^{3\alpha_3(c)} \\
&= \sum_{c \in C} X^{3\alpha_0(c) + 2\alpha_1(c) + \alpha_2(c)} Y^{\alpha_1(c) + 2\alpha_2(c) + 3\alpha_3(c)} \\
&= \sum_{c \in C} X^{3n - w_L(c)} Y^{w_L(c)} \\
&= Lee_C(X, Y).
\end{aligned}$$

2. From the definition of symmetrized weight enumerator, we have

$$\begin{aligned}
cwe_C(X, Y, Y, Y) &= \sum_{c \in C} X^{\alpha_0(c)} Y^{\alpha_1(c)} Y^{\alpha_2(c)} Y^{\alpha_3(c)} \\
&= \sum_{c \in C} X^{\alpha_0(c)} Y^{\alpha_1(c) + \alpha_2(c) + \alpha_3(c)} \\
&= \sum_{c \in C} X^{n - w_H(c)} Y^{w_H(c)} \\
&= Ham(X, Y).
\end{aligned}$$

3. From the definition of Lee weight enumerator, we can obtain

$$\begin{aligned}
Lee_C(X, Y) &= \sum_{\Psi(c) \in \Psi(C)} X^{3n - w_L(\Psi(c))} Y^{w_L(\Psi(c))} \\
&= w_{\Psi(C)}(X, Y).
\end{aligned}$$

4. From theorem 6, we have $\Psi(C)^\perp = \Psi(C^\perp)$, and they are linear codes from Lemma 5, we have

$$w_{\Psi(C^\perp)}(X, Y) = \frac{1}{|\Psi(C)|} w_{\Psi(C^\perp)}(X + Y, X - Y).$$

On the other hand, since $|\Psi(C)| = |C|$, and by 3 in this theorem, we have

$$\begin{aligned}
Lee_{C^\perp}(X, Y) &= w_{\Psi(C^\perp)}(X, Y) \\
&= \frac{1}{|\Psi(C)|} w_{\Psi(C^\perp)}(X + Y, X - Y) \\
&= \frac{1}{|C|} Lee_C(X + Y, X - Y).
\end{aligned}$$

□

5 Cyclic Codes over R

Cyclic codes play a very important role in the coding theory. We give in this section some useful results on cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ is said to be cyclic if it satisfies:

$$(c_{n-1}, c_0, \dots, c_{n-2}) \in C \text{ whenever } (c_0, c_1, \dots, c_{n-1}) \in C.$$

It is well known that cyclic codes of length n over R can be identified with an ideal in the quotient ring $R[x]/\langle x^n - 1 \rangle$ via the R -module isomorphism as follows:

$$\begin{aligned} R^n &\rightarrow R[x]/\langle x^n - 1 \rangle \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1} \end{aligned}$$

Theorem 5.1 *A linear code $C = vC_1 \oplus (1-v)C_2 \oplus (1-v^2)C_3$ is cyclic over R if and only if C_1 , C_2 , and C_3 are cyclic codes of length n over \mathbb{F}_q .*

Proof. Let $(a_0, a_1, \dots, a_{n-1}) \in C_1$, $(b_0, b_1, \dots, b_{n-1}) \in C_2$ and $(d_0, d_1, \dots, d_{n-1}) \in C_3$. suppose that $c_i = va_i + (1-v)b_i + (1-v^2)d_i$ for $i = 0, 1, \dots, n-1$. Since C is a cyclic code, it follows that $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$. Note that $(c_{n-1}, c_0, \dots, c_{n-2}) = v(a_{n-1}, a_0, \dots, a_{n-2}) + (1-v)(b_{n-1}, b_0, \dots, b_{n-2}) + (1-v^2)(d_{n-1}, d_0, \dots, d_{n-2})$. Hence $(a_{n-1}, a_0, \dots, a_{n-2}) \in C_1$, $(b_{n-1}, b_0, \dots, b_{n-2}) \in C_2$ and $(d_{n-1}, d_0, \dots, d_{n-2}) \in C_3$, which implies that C_1 , C_2 , and C_3 are cyclic codes over \mathbb{F}_q . Conversely, suppose that C_1 , C_2 , and C_3 are cyclic codes over \mathbb{F}_q . Let $(c_0, c_1, \dots, c_{n-1}) \in C$, where $c_i = va_i + (1-v)b_i + (1-v^2)d_i$ for $i = 0, 1, \dots, n-1$. Then $(a_0, a_1, \dots, a_{n-1}) \in C_1$, $(b_0, b_1, \dots, b_{n-1}) \in C_2$ and $(d_0, d_1, \dots, d_{n-1}) \in C_3$. Note that $(c_{n-1}, c_0, \dots, c_{n-2}) = v(a_{n-1}, a_0, \dots, a_{n-2}) + (1-v)(b_{n-1}, b_0, \dots, b_{n-2}) + (1-v^2)(d_{n-1}, d_0, \dots, d_{n-2})$. Therefore, C is a cyclic code over R . \square

Corollary 5.2 *Let $C = vC_1 \oplus (1-v)C_2 \oplus (1-v^2)C_3$ be cyclic code of length n over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, then its dual code C^\perp is also cyclic and moreover we have $C^\perp = vC_1^\perp \oplus (1-v)C_2^\perp \oplus (1-v^2)C_3^\perp$.*

Corollary 5.3 *There exists a self-dual cyclic code of length n over R if and only if q is power of 2 and n is even.*

Proof. We know that $C = vC_1 \oplus (1-v)C_2 \oplus (1-v^2)C_3$. From [10, Theorem 1] we have C_1 , C_2 and C_3 are self-dual cyclic code over \mathbb{F}_q if and only if q is power of 2 and n is even. Then we have the result of C . \square

Theorem 5.4 *Let $C = vC_1 \oplus (1-v)C_2 \oplus (1-v^2)C_3$ be a cyclic code of length over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, then $C = \langle vC_1, (1-v)C_2, (1-v^2)C_3 \rangle$, where $C_i = \langle f_i \rangle$, $f_i \in \mathbb{F}_q$ ($i = 1, 2, 3$), $f_i / \langle x^n - 1 \rangle$, and $|C| = q^{3n - (\deg f_1 + \deg f_2 + \deg f_3)}$.*

Proof. Assuming that $C_i = \langle f_i \rangle, f_i \in \mathbb{F}_q, |C_i| = q^{n-\deg f_i} (i = 1, 2, 3)$. It is obvious that $C \subseteq \langle v f_1, (1-v) f_2, (1-v^2) f_3 \rangle$. Now, let $r = v f_1 r_1 + (1-v) f_2 r_2 + (1-v^2) f_3 r_3 \subseteq \langle v f_1, (1-v) f_2, (1-v^2) f_3 \rangle$, where $r, r_i \in (\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q)[x], i = 1, 2, 3$. So there exists $a_0, a_1, a_2 \in \mathbb{F}_q[x]$ such that $r_i = v f_1 a_1 + (1-v) f_2 a_2 + (1-v^2) f_3 a_3$. Hence $r = v f_1 r_1 + (1-v) f_2 r_2 + (1-v^2) f_3 r_3 = v f_1 a_1 + (1-v) f_2 a_2 + (1-v^2) f_3 a_3 \in C$. That is $\langle v f_1, (1-v) f_2, (1-v^2) f_3 \rangle \subseteq C$. \square

6 Formally Self-Dual Codes over R

Formally self-dual binary codes are extensively studied codes. This class of codes plays a very significant role in coding theory both from partial a theoretical points of view.

We study in this section the different methods construction of formally self-dual codes over R .

A code is called self-dual if $C = C^\perp$. It is called isodual if C is equivalent to C^\perp . The code C is called formally self-dual if $w_C(y) = w_{C^\perp}(y)$.

And here we present three kinds of construction methods for formally self-dual over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ Specially we obtain the following results.

Theorem 6.1 (consrtuction A) *Let A be an $n \times n$ matrix over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ such $A^T = A$. Then the code generated $G = [I_n | A]$ is an isodual code and hence a formally self-dual code of length $2n$.*

Proof. Let

$$G = [I_n | A]$$

$$G = \begin{pmatrix} 1 & 0 & \dots & 0 & A_{11} & A_{12} & \dots & A_{1n} \\ 0 & 1 & \dots & 0 & A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix}$$

The matrix generated of type $2n \times n$.

And consider the matrix

$$\acute{G} = [-A^T | I_n]$$

$$\acute{G} = \begin{pmatrix} -A_{11} & -A_{21} & \dots & -A_{n1} & 1 & 0 & \dots & 0 & 0 \\ -A_{12} & -A_{22} & \dots & -A_{n2} & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ -A_{1n} & -A_{2n} & \dots & -A_{nn} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \text{ of type } 2n \times n.$$

G and \acute{G} generate codes with free rank $k \times n$. We need to show that $\acute{C} = C^\perp$. Let u the first row of G and let v the first row of \acute{C} , we have $\langle u, v \rangle = A_{11} - A_{11} = 0$.
for u the first row of G and j -th row of \acute{G} , we have $\langle u, v \rangle = A_{1n} - A_{1n} = 0$. For u the i -th row of G and j -th row of \acute{G} we have $\langle u, v \rangle_k = A_{ij} - A_{ji} = 0$. Since $A^T = A$. There for $\acute{C} = C^\perp$ and C is equivalent to C^\perp . Since $w_L(-a) = w_L(a)$ for all $a \in \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, this is a weight preserving equivalence. □

Example 6.2 Let $q = 3$ and $n = 5$ and A be the matrix

$$A = \begin{pmatrix} 0 & v & 2+v & 1+2v+2v^2 & 2v+2v^2 \\ v & 2v+2v^2 & 2 & 1+v & 1+v^2 \\ 2+v & 2 & 2v^2 & 2+v+v^2 & 1+2v \\ 1+2v+v^2 & 1+v & 2+v+v^2 & 1 & v \\ 2v+2v^2 & 1+v^2 & 1+2v & v & 2 \end{pmatrix}$$

we have $A = A^\top$. Then $[I_5 | A]$ generates a formally self-dual code of length 10 over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and the Gray image of the code is a $[30, 15, 9]_3$ formally self-dual.

Theorem 6.3 (construction B) Let M be a circulant matrix over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ of order n . Then $G = (I_n | M)$ generates an isodual code and hence a formally self-dual code over R . This is called the double circulant construction.

Proof. Consider

$$M = \begin{pmatrix} M_{11} & M_{12} & \dots & M_{1n} \\ M_{1n} & M_{11} & \dots & M_{1n-1} \\ \vdots & \vdots & \vdots & \vdots \\ M_{12} & M_{13} & \dots & M_{11} \end{pmatrix}$$

the circulant matrix over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ of $n \times n$.

Let

$$G = (I_n | M)$$

$$G = \begin{pmatrix} 1 & 0 & \dots & 0 & M_{11} & M_{12} & \dots & M_{1n} \\ 0 & 1 & \dots & 0 & M_{1n} & M_{11} & \dots & M_{1n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & M_{12} & M_{13} & \dots & M_{11} \end{pmatrix} \text{ of type } 2n \times n$$

And let

$$\acute{G} = (-M^T | I_n)$$

$$\dot{G} = \begin{pmatrix} -M_{11} & -M_{1n} & \dots & -M_{12} & 1 & 0 & \dots & 0 \\ -M_{12} & -M_{11} & \dots & -M_{13} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ -M_{1n} & -M_{1n-1} & \dots & -M_{11} & 0 & 0 & \dots & 1 \end{pmatrix} \text{ of type } 2n \times n$$

When C code generated by G , and \dot{C} generated by \dot{G} . It can similarly be shown that $\dot{C} = C^\perp$ is equivalent over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ to be code C'' . There is a permutation of rows such that after applying it to C'' , the first column of $\sigma(M^T)$ is the same as the first column of M . Namely:

$$(M_{11}, M_{21}, \dots, M_{n1}) = (M_{\sigma(1)1}^T, M_{\sigma(2)1}^T, \dots, M_{\sigma(n)1}^T) = (M_{1\sigma(1)}, M_{1\sigma(2)}, \dots, M_{1\sigma(n)}).$$

Since the matrix M is circulant, every column of M is then equal to a column of $\sigma(M^T)$. Then apply the necessary column permutation τ so that $\tau(\sigma(M^T)) = M$. We apply another column permutation ρ so that $\sigma(I_n) = I_n$. Which means that C is equivalent to $\dot{C} = C^\perp$, hence the codes are isodual. \square

Example 6.4 Let $q = 5$ and $n = 5$ and M be a circulant matrix

$$M = \begin{pmatrix} 3v + 2v^2 & 4v & 3 + 2v & 1 + 2v + 2v^2 & 2v + 3v^2 \\ 2v + 3v^2 & 3v + 2v^2 & 4v & 3 + 2v & 1 + 2v + 2v^2 \\ 1 + 2v + 2v^2 & 2v + 3v^2 & 3v + 2v^2 & 4v & 3 + 2v \\ 3 + 2v & 1 + 2v + 2v^2 & 2v + 3v^2 & 3v + 2v^2 & 4v \\ 4v & 3 + 2v & 3 + 2v & 1 + 2v + 2v^2 & 2v + 3v^2 \end{pmatrix}$$

Then $[I_5 | M]$ generates a formally self-dual code of length 10 over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and the Gray image of the code is a $[30, 15, 12]_5$ formally self-dual.

Theorem 6.5 (construction C) Let M be a circulant matrix over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ of order $n - 1$. Then the matrix

$$G = \left(I_n \left| \begin{array}{cccc} \alpha & \omega & \dots & \omega \\ \omega & & & \\ \vdots & & M & \\ \omega & & & \end{array} \right. \right)$$

Where $\alpha, \omega \in \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, is generator matrix of a formally self-dual code over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$.

Proof. For

$$M = \begin{pmatrix} M_{11} & M_{12} & \dots & M_{1n-1} \\ M_{1n-1} & M_{11} & \dots & M_{1n-2} \\ \vdots & \vdots & \ddots & \vdots \\ M_{12} & M_{13} & \dots & M_{11} \end{pmatrix}$$

we have

$$G = \begin{pmatrix} 1 & 0 & \dots & 0 & \alpha & \omega & \dots & \omega \\ 0 & 1 & \dots & 0 & \omega & M_{11} & \dots & M_{1n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \omega & M_{12} & \dots & M_{11} \end{pmatrix}$$

Where $\alpha, \omega \in \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$.

And consider \dot{G} be given as

$$\dot{G} = \begin{pmatrix} -\alpha & -\omega & \dots & -\omega & 1 & 0 & \dots & 0 \\ -\omega & -M_{11} & \dots & -M_{12} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -\omega & -M_{1n-1} & \dots & -M_{11} & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Let $C = \langle G \rangle$ and $\dot{C} = \langle \dot{G} \rangle$. Both C and \dot{C} are codes of free rank n . Let v be the first row of G , and let w be the j -th row of \dot{G} . We have $\langle u, v \rangle_k = w - w = 0$. Let v be the i -th row of G , and let w be the j -th row of \dot{G} . We have $\langle u, v \rangle_k = M_{ij} - M_{ij} = 0$. Hence C and $\dot{C} = C^\perp$.

We see that C and \dot{C} have the same weight enumerator. Hence C and C^\perp have the same weight enumerators.

Example 6.6 Let $q = 3$ and $\alpha = 2 + v + 2v^2$ and $\omega = 2 + 2v$ and $n = 4$ and M be a circulant matrix of order $n - 1 = 3$

$$M = \begin{pmatrix} 2 & 1 + v & 2v^2 \\ 2v^2 & 2 & 1 + v \\ 1 + v & v^2 & 2 \end{pmatrix}$$

then

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 + v + 2v & 2 + 2v & 2 + 2v & 2 + 2v \\ 0 & 1 & 0 & 0 & 2 + 2v & 2 & 1 + v & 2v^2 \\ 0 & 0 & 1 & 0 & 2 + 2v & 2v^2 & 2 & 1 + v \\ 0 & 0 & 0 & 1 & 2 + 2v & 1 + v & 2v^2 & 2 \end{pmatrix}$$

generates a formally self-dual code of length 10 over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and the Gray image of the code is a $[24, 12, 9]_3$ formally self-dual.

□

7 The Gray Image of Formally Self-Dual Codes

Self-dual codes are by definition formally self-dual automatically. There exists formally self-dual codes which are not self-dual. In this section, we study formally self-dual codes over rings with a Gray map.

A code is called even if the weights of all codewords are even, in otherwise the code is called odd.

Theorem 7.1 *If C is a formally self-dual codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ then the image under the corresponding Gray map is formally self-dual code.*

Proof. Follow from theorem 6. Since self-dual codes are formally self-dual. \square

Lemma 7.2 *The direct product of formally self-dual codes over a ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ is a formally self-dual code.*

Proof. Let C_1 and C_2 be formally self-dual codes it follows that $w_{C_1}(y) = w_{C_1^\perp}(y)$ and $w_{C_2}(y) = w_{C_2^\perp}(y)$. Then

$$\begin{aligned} w_{C_1 \times C_2}(y) &= w_{C_1}(y) w_{C_2}(y) \\ &= w_{C_1^\perp \times C_2^\perp}(y) \\ &= w_{C_1^\perp}(y) w_{C_2^\perp}(y) \end{aligned}$$

Notice that $(C_1 \times C_2)^\perp = C_1^\perp \times C_2^\perp$, we have that $C_1 \times C_2$ is formally self-dual code. \square

Theorem 7.3 *Linear odd formally self-dual codes exist over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ for all lengths.*

Proof. Notice there are linear odd formally self-dual code of length 1, so by previous theorem taking direct products of this code we exit with a result that there are odd formally self-dual of all length. \square

References

- [1] A. Bayram, I.Siap, Cyclic and constacyclic codes over a non-chain ring, J.Algebra Comb. Discrete App. 1(1). 1-12.
- [2] A. Batoul, K. Guenda, A. Kaya, B. Yildiz, Cyclic isodual and formally self-dual codes over $\mathbb{F}_q + v\mathbb{F}_q$, EJPAM. Vol. 8, No. 1, 2015, 64-80.
- [3] A. Dertli. Y. Cengellenmis, S. Eren, On Quantum Codes Obtained From Cyclic Codes Over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$, arXiv: 1407. 1232v1[cs.IT] 19 jun 2014.

- [4] S. T.Dougherty, Formally self-dual codes and Gray maps, Thirteenth International Workshop on Algebraic and Combinatorial coding Theory June 15-21, 2012, Pomorie, Bulgaria.
- [5] M.Jia, P.Solé and B. Wu, Cyclic Codes and the Weight Enumerator of Linear Codes over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$, App. Comput. Math, V. 12, N 2, 2013.
- [6] A.Kaya, B. Yildiz, I. Siap, Quadratic Residue Codes Over $\mathbb{F}_p + v\mathbb{F}_p$ And Their Gray Images, arXiv: 1305. 4508v1[cs.IT] 20 May 2013.
bibitemkaradeniz S. karadeniz, S. T.Dougherty, Construction formally self-dual codes over R_k . May 21, 2013.
- [7] D. Liao, Y.Tang, A Class Of Constacyclic Codes Over $R + vR$ and Its Gray Image, Int. J. Communication, Network and System Sciences, 2012, 5, 222-227.
- [8] S. Zhu, L. Wang, A class of constracyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image, Discrete Mathematics 311(2011) 2677-2682.
- [9] Y. Liu, M. Shi, P. Solé, Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, MSC(2010): Primary 94B15; Secondary 11A15.
- [10] Y. Jia, S. Ling and C. Xing, On Self-Dual Cyclic Codes over Finite Fields. IEEE transactions on information theory, Vol 57, O 4, April 2011.